Incident Response
Table Top Training

Battle Testing Incident Response Teams

Incident Response is a highly-skilled discipline that demands participation from personnel inside and sometimes outside the organization. To that end, ensuring responders are able to execute their roles and properly communicate with team members is critical and requires practice that needs to be performed before facing a cyber related incident.

Cylance® Consulting's Incident Response Table Top Training provides the education your staff needs to **effectively carry out your incident response plan**. Your incident response team will **leave with the knowledge of how to work together across the established roles and tasks necessary to defend against a security incident**. Organization leadership will gain an increase in assurance of internal incident response team member capabilities while improving team interaction across the organization, including how to efficiently work with C-Level, legal, technical personnel, uncooperative staff and personnel who may lack experience with security incident management.

Service Overview

Cylance Consulting's IR Table Top Exercise service seeks input from your organization to gain a broad understanding of the intricacies and capabilities that apply to your environment. Cylance Consulting will engage in an information gathering exercise to ensure key environmental factors are included in the scenarios to help develop injects that help drive the event simulations, challenge participants, and test performance under pressure. Customized table top training will be conducted to ensure IR team members understand their roles and responsibilities as well as how they will interact and communicate with other team members.

Table Top Training will cover the key phases of an Incident Response Plan to include nuances unique to your organization and potential threats, which may include:

- Insider Threat
- Malware / Ransomware
- Social Engineering
- Business Email Compromise
- Unauthorized Access
- Distributed Denial of Service
- Web Application Attack / Outage
- Advanced Persistent Threat

Benefits:

- Sessions tailored towards your organization's unique environments

- Team members learn how to establish and fortify an organization's security and incident response capabilities

- Detailed playbooks incorporating the current IR process and employee roles are developed

- The experience of world renowned incident response experts is leveraged to build and enhance your IR plan

- Team members and management staff gain confidence

77%
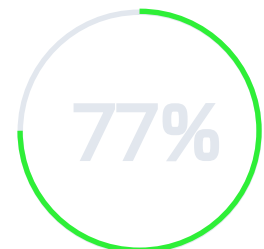
Ransomware volume has increased by 350% since 2016. Ransomware now accounts for nearly 24% of malware-related security incidents.

Source: Ponemon Institute, 2018 Cyber Resilient Organizations

Incident Response Table Top Training Phases and Duration*		
Phase 1	Documentation Review & Interviews	2-3 weeks depending on scope
Phase 2	Development and Review of Exercise Scenarios	1-2 weeks depending on scope
Phase 3	On Site Tabletop Training	1 day
Phase 4	Observations and Recommendations Report Development	2-3 weeks depending on scope
Phase 5	Reviews, Revisions, and Final Presentation	1-2 weeks depending on scope

Schedule is an example time frame and may vary.

Deliverables

As part of the training exercise, Cylance Consulting will:

- Conduct on-site table top training sessions for technical and management employees, and larger, unified training session for the entire team

- Provide a Formal Observations and Recommendations Report

- Provide a Formal Observations and Recommendations Executive Presentation

Prepare your incident response teams with the specialized skills and knowledge needed to respond to an incident. Contact Cylance Consulting or your technology provider to discuss your training needs.

About Cylance Consulting

- World-renowned experts combine subject matter experts from different practice areas to deliver consistent, fast, and effective services around the world

- Incorporates artificial intelligence into tools and back end data analysis processes to more efficiently and effectively secure the environment and *prevent* attacks

- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization

- Techniques are designed to not impact operations in any way

- Integrated practice areas: ThreatZERO™ Services, Incident Containment, and Compromise Assessments, Red Team Services, Industrial Control Systems Security, IoT and Embedded Systems, and Education

::: BlackBerry®
CYLANCE®

+1-877-973-3336
proservices@cylance.com
www.cylance.com/consulting